

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles

de Terwangne , Cécile

Published in:
Petites Affiches

Publication date:
2005

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

de Terwangne , C 2005, 'Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles', *Petites Affiches*, Numéro 194, p. 4-55.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles

**Prof. Cécile de Terwangne
FUNDP – CRID
Namur**

Alors que pendant des dizaines d'années, les décisions prononcées par les cours et tribunaux ont été publiées dans des revues ou périodiques spécialisés, sur support papier, depuis plus de vingt ans la diffusion de la jurisprudence s'effectue également sur support électronique. Le phénomène est en croissance. On a vu fleurir, du fait d'acteurs publics et privés, des bases de données jurisprudentielles distribuées sur CD-ROM ou via des abonnements en ligne et, plus récemment, accessibles via internet. Initialement réservés aux professionnels du droit, ces outils documentaires sont aujourd'hui à la portée de tous. Les qualités du support électronique permettent de mettre à disposition une quantité de décisions largement supérieure aux possibilités du support papier tout en fournissant les instruments de recherche, de sélection et d'extraction sans lesquels un réel accès à l'information ne serait pas possible. Cette évolution doit-elle conduire à revoir les équilibres atteints pour la publication papier entre intérêt de la publication et intérêt des personnes nommément citées dans les jugements et arrêts ?¹

1. L'application de la législation de protection des données personnelles à la publication des décisions de jurisprudence sur internet

La mise à disposition du public d'un jugement contenant des données sur des personnes physiques (qu'il s'agisse du juge, du Ministère public, des plaideurs, des parties, de témoins, etc.) correspond à un traitement de données à caractère personnel au sens de la directive 95/46/CE garantissant la protection des données personnelles². En effet, la simple mention du nom d'une personne physique ou de caractéristiques permettant d'identifier un individu fait intervenir des données à caractère personnel définies comme « toute information se rapportant à une personne physique identifiée ou identifiable »³. Par ailleurs, diffuser une décision de justice comportant de telles données implique une opération effectuée sur des données à caractère personnel et, partant, un traitement de données⁴.

¹ Cette contribution est centrée pour l'essentiel sur la mise à disposition des bases de données de jurisprudence et n'évoque qu'incidemment la publication des décisions de justice par la presse. On ne trouvera pas dans ces pages l'analyse systématique du régime juridique de ces dernières publications.

² Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O. L* 281, 23 novembre 1995, p. 31.

³ Art. 2, a), de la directive 95/46.

⁴ Par « traitement de données à caractère personnel », l'article 2, b), de la directive 95/46 entend : « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

En tant que traitement de données à caractère personnel, la publication des décisions de justice non anonymisées tombe sous le coup de la directive 95/46 dans l'hypothèse où la diffusion se réalise sur support électronique ; c'est le cas d'une diffusion sur CD-Rom ou via un site web, par exemple.

La directive de protection des données, ou plus exactement les lois nationales qui l'ont transposée ainsi que le règlement adopté sur sa base pour y soumettre les institutions communautaires, sont donc applicables à l'hypothèse qui retient l'attention dans cette contribution, c'est-à-dire la mise à disposition de décisions de jurisprudence par la voie d'internet. Il convient dès lors d'analyser les implications juridiques découlant de l'application du régime de protection des données à cette hypothèse et d'observer les formes qu'elles ont prises dans les différents Etats membres de l'Union européenne.

La protection mise en place repose sur trois principes fondamentaux : principes de finalité, de proportionnalité et de transparence. Nonobstant, une protection spécifique, renforcée, est accordée aux données qualifiées de sensibles au regard de leur nature, au titre desquelles on trouve les données « judiciaires ». Les pages qui suivent s'attachent à vérifier les conséquences des deux premiers principes et du régime de protection spécifique réservé aux données « judiciaires » sur la publication de la jurisprudence au travers d'internet et d'observer les situations dans les Etats membres – anonymisation obligatoire ou à la demande, ou diffusion libre – qui en ont résulté.

2. Les exigences découlant du principe de finalité

Principe clé de la protection, le principe de finalité exige que tout traitement poursuive une ou des finalité(s) déterminée(s) et légitime(s) (point 2.1.), que l'on ne fasse que ce qui est compatible avec cette (ces) finalité(s) (point 2.2.) et que l'on ne traite que les données pertinentes au vu de la (des) finalité(s) (point 2.3.).

Il est donc de première importance de s'interroger sur les finalités poursuivies par la mise à disposition du public des décisions de jurisprudence.

2.1. Les finalités liées à la mise à disposition des décisions de jurisprudence

Au premier rang des finalités rapidement avancées figure la transparence de la justice, devant permettre de lutter contre l'arbitraire. Il ne faut toutefois pas confondre ou assimiler publicité et publication des décisions de justice.

L'article 6 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales garantissant le droit à un procès équitable rattache à ce droit le prononcé public des décisions de justice. Cet article dispose que

« Toute personne a droit à ce que sa cause soit entendue équitablement et publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial (...). Le jugement doit être rendu publiquement mais l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique, lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent, ou dans une mesure

jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice. ».

Le caractère par principe public de la procédure et de la décision de justice garantit la confiance du public dans la probité du système judiciaire et favorise la compréhension de l'administration de la justice. A l'occasion de l'adoption, en Belgique, de l'arrêté royal imposant la publication des arrêts du Conseil d'Etat par la voie d'internet, le ministre de l'Intérieur signalait : « [La publicité donnée aux décisions de justice] protège indirectement mais efficacement le juge contre les influences extérieures qui pourraient affecter de manière inconvenante le droit qui lui appartient de juger. Toute décision du juge doit en effet non seulement être logique et légalement justifiée en soi, mais, en outre, pouvoir être mise à l'épreuve, au regard de ces exigences, par toute personne susceptible de relever de ce pouvoir de juger. »⁵

De l'obligation de publicité des prononcés découle le droit du public de consulter les décisions conservées par les greffes des tribunaux, ainsi que le droit de la presse de rendre compte des décisions constituant l'actualité judiciaire du moment.

C'est le caractère public des prononcés qui légitime par ailleurs la publication des décisions de jurisprudence dans des revues juridiques ou des compilations de jurisprudence. Cette publication ne réalise pas elle-même la publicité des décisions de justice, même si elle contribue à porter ces dernières à la connaissance du public. Ce n'est pas de la publication de la jurisprudence que dépend la protection contre l'arbitraire des juges et le caractère équitable des procès. Si c'était le cas, il faudrait nourrir de vives inquiétudes pour la très grande majorité de la jurisprudence qui ne fait l'objet d'aucune publication...^{6,7} Cela étant, il est clair que même si elle ne vise pas à garantir la publicité de la justice, la publication des décisions de jurisprudence présente l'« avantage collatéral » d'induire une forme de contrôle de la qualité du travail des juges. En cela, elle contribue sans nul doute à la protection du justiciable contre l'arbitraire. Plus la probabilité est grande pour le juge de voir sa décision publiée et dès lors soumise à la critique, plus il sera vigilant, on imagine, quant à la rigueur du raisonnement tenu et de sa formulation.

La publication de la jurisprudence, quelle que soit la forme qu'elle prend, classique sur papier ou électronique sur CD-ROM ou sur internet, poursuit le but de faire connaître à tout intéressé la dimension « vécue » du droit, souvent révélatrice de la véritable portée des textes normatifs, voire même créatrice de droit. A ce but se greffe immédiatement celui « d'alimenter la discussion sur la jurisprudence comme source de droit »⁸. Il ne s'agit nullement de viser à « porter à la connaissance le bon droit ou la condamnation de telle ou

⁵ Rapport au Roi précédant l'arrêté royal du 7 juillet 1997 relatif à la publication des arrêts du Conseil d'Etat, *Mon. B.*, 8 août 1997, p. 20239.

⁶ Sur les 930.000 décisions de tous types prononcées en Belgique en 2003 (chiffre communiqué par le ministère belge de la Justice, <http://www.just.fgov.be>), seules approximativement 5.000 ont eu droit à une publication...

⁷ En Espagne, certains auteurs ont souligné que la mise à disposition des jugements et arrêts réalisée par le *Centro de Documentacion Judicial*, organisme indépendant chargé de sélectionner et diffuser l'information juridique, législative, jurisprudentielle et doctrinale, ne pouvait en aucun cas remplacer le principe de la publicité des jugements. Ces auteurs ont mis en exergue qu'il est important d'assurer l'accès des citoyens aux jugements dans leur forme originale, c'est-à-dire non anonymisés, tels qu'ils sont conservés auprès des tribunaux, en parallèle de la mise à disposition par le biais du centre de documentation. Voy. les auteurs cités par Rosario Duaso-Calès, *La protection des données personnelles contenues dans les documents publics accessibles sur Internet : le cas des données judiciaires*, Mémoire, Faculté de Droit, Université de Montréal, 2002, p. 146.

⁸ Commission belge de la protection de la vie privée, avis n° 42/97 du 23 décembre 1997 relatif à la diffusion des décisions juridictionnelles par le recours aux technologies de l'information et de la communication, disponible à l'adresse <http://www.privacy.fgov.be>.

telle personne »⁹. Le *Garante per la protezione dei dati personali*, autorité de contrôle italienne, a spécifié dans le même sens que la collecte et la diffusion de données à caractère judiciaire, en particulier les données relatives aux décisions jurisprudentielles, poursuit des finalités de « documentation, étude et recherche dans le champ juridique »¹⁰.

La Recommandation R (95) 11 du Conseil de l'Europe, du 11 septembre 1995, relative à la sélection, au traitement, à la présentation et à l'archivage des décisions judiciaires dans les systèmes de documentation juridiques automatisés énonce d'ailleurs solennellement que « la pleine connaissance de la jurisprudence de toutes les juridictions est une des conditions essentielles de l'application équitable du droit ». Le Comité des Ministres du Conseil de l'Europe, auteur de cette recommandation, a identifié les objectifs attachés aux systèmes automatisés de diffusion de la jurisprudence. On observera que, dans le même sens que ce qui est dit plus haut, la transparence de la justice et la garantie contre l'arbitraire des juges ne sont pas repris en tant que tels comme objectifs de cette diffusion. Les objectifs sont, selon le Comité des Ministres,

- de faciliter la tâche des professions juridiques en fournissant des renseignements prompts, complets et à jour ;
- de renseigner toute personne intéressée par une question de jurisprudence ;
- de rendre publiques plus rapidement des décisions nouvelles, particulièrement dans les domaines du droit en évolution ;
- de rendre publiques un plus grand nombre de décisions intéressant tant le domaine normatif que le domaine factuel (quantum des indemnités, des pensions alimentaires, des peines, etc.) ;
- de contribuer à la cohérence de la jurisprudence (sécurité de droit – « *Rechtssicherheit* ») sans toutefois introduire de rigidité ;
- de permettre au législateur de faire des analyses de l'application des lois ;
- de faciliter les études sur la jurisprudence ;
- dans certains cas, de fournir des informations à des fins statistiques.¹¹

2.2. Des utilisations compatibles avec les finalités de diffusion. Interdiction des détournements de finalité

Le principe de finalité impose que l'on n'utilise les données personnelles qu'en vue de réaliser les finalités liées au traitement des données (le traitement étant, dans le cas qui nous occupe, la diffusion des décisions de jurisprudence). Il est interdit de détourner la finalité et de traiter les données dans un but incompatible avec le but initial¹².

Or, la publication des décisions de jurisprudence sur support électronique permet techniquement, et en conséquence offre la tentation, de consulter les bases de données dans un

⁹ *Ibidem*.

¹⁰ Autorisation n° 7 de 2002 relative au traitement des données à caractère judiciaire, disponible à l'adresse <http://www.garanteprivacy.it>.

¹¹ Annexe 1 à la Recommandation n° R (95) 11, intitulée Principes généraux pour les systèmes de documentation juridique automatisés concernant la sélection, le traitement, la présentation et l'archivage des décisions de justice.

¹² Art. 6, § 1^{er}, b) de la directive 95/46.

but différent de celui d'être éclairé sur un courant jurisprudentiel dans une matière particulière. Le Groupe des responsables de la protection des données européens établi par l'article 29 de la directive signale, dans son avis 3/99 : « Instruments de documentation juridique, les bases de données jurisprudentielles peuvent devenir [...] des fichiers de renseignements sur les personnes si on les consulte [...] pour obtenir toutes les décisions de justice se rapportant à une même personne »¹³. La Commission Nationale de l'Informatique et des Libertés (CNIL) française relève dans le même sens, dans sa Délibération portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence : « ce qui est techniquement possible lorsqu'une recherche documentaire via internet est entreprise [...] l'est aussi lorsqu'il s'agit de se renseigner sur un candidat à l'emploi, à un logement ou à un crédit, sur un voisin ou un proche et ce, à l'insu des personnes concernées »¹⁴.

A l'instar de la CNIL, la Commission belge de la protection de la vie privée a marqué sa préoccupation pour la question. Dans son avis du 22 avril 1996, elle note : « Les recherches automatisées habituelles dans du texte libre, disponibles dans les logiciels de consultation des CD-ROM ou des réseaux comme Internet, permettent, en effet, d'opérer des sélections dans de vastes recueils de prononcés sur la base des noms des parties, en combinaison avec d'autres critères de recherche, dont on peut déduire de façon systématique des informations concernant la vie privée des personnes identifiées »¹⁵. Ainsi, la constitution et la mise à disposition d'une base de données jurisprudentielles permet de recueillir « l'ensemble de la jurisprudence relative à des licenciements pour motifs graves, pour en extraire les noms et adresses des employés mis en cause » ou d'identifier « aisément les médecins dont la responsabilité aura été poursuivie devant les tribunaux. »^{16 17}.

Parmi d'autres organes de protection et de contrôle opérant sur le sol européen, signalons encore les mots d'un commissaire allemand à la protection des données stigmatisant les dangers d'utilisation détournée liés à une publication sur internet : « [...] reports about convictions long after the sentence has been served are published in multimedial forms, usable for surveillance, credit information or other purposes related to civil life and accessible worldwide ».¹⁸

¹³ Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, avis 3/99 du 3 mai 1999 concernant l'information émanant du secteur public et la protection des données à caractère personnel, p. 7, http://europa.eu.int/comm/internal_market/eu/media/dataprot/wpdocs/wp20/fr.pdf

¹⁴ CNIL, Délibération 01-057 du 29 novembre 2001.

¹⁵ Avis 07/98, disponible à l'adresse www.privacy.fgov.be

¹⁶ Y. POULLET, « Autour de l'arrêté royal du 7 juillet 1997 relatif à la publication des arrêts du Conseil d'Etat : les technologies de l'information et de la communication, une solution à la pathologie législative ? », in *La pathologie législative, comment en sortir ?*, coll. Droit en Mouvement, Bruxelles, La Charte, 1998, p. 70. Voy. également A. PERDRIAU, « L'anonymisation des jugements civils », *J.C.P.*, éd. G, 1999, I, 163, pp. 1615-1616.

¹⁷ Claude Bourgeois évoque les « sociétés qui ont pour activité principale la constitution de 'mégabases' de données nominatives qu'elles revendent à des sociétés commerciales telles que les assurances, les établissements de crédit, les agences de travail intérimaire ou les agences immobilières... Or [ces sociétés] pourraient être très intéressées par des données concernant les personnes s'étant trouvées par le passé dans une situation de surendettement, ayant eu un litige avec leur bailleur ou ayant été licenciées pour faute grave... » (« Réflexions à propos de l'anonymisation des décisions de justice publiées sur support numérique », *Communication – Commerce électronique*, 2004, n° 6, p. 17).

¹⁸ S. WALZ, « Relationship between the freedom of the press and the right to informational privacy in the emerging Information Society », contribution présente à la 19^{ème} Conférence internationale des Commissaires à la protection des données, Bruxelles, 17-19 septembre 1997, p. 3.

Face à de tels risques de détournements, le *Garante per la protezione dei dati personali* italien a lancé fermement un appel au respect du principe de finalité, dans son avis concernant la réglementation de l'accès à la base de données de la Cour de cassation¹⁹. Le *Garante* énonce qu'il n'est pas permis d'utiliser les données contenues dans cette base de données à des fins de création de profils de juges ou de sujets condamnés. La Commission belge de la protection de la vie privée a estimé, elle, à la suite de son constat repris ci-dessus, qu'il fallait faire preuve d'une plus grande retenue dans la mention des données pouvant mener à l'identification des parties dans les chroniques automatisées de jurisprudence, par rapport aux publications papier et qu'il fallait renoncer à indexer les décisions de justice à partir du nom des parties, afin d'interdire les recherches à partir de ce critère²⁰. La CNIL a conclu de façon générale pour la publication de données personnelles sur internet, que les risques de perte de contrôle sur ses données, accompagnés des risques de détournement de finalités d'utilisation, sont tels que la seule manière de rétablir l'équilibre entre le droit au respect de la vie privée et l'intérêt de la publicité consiste à obtenir des personnes concernées leur consentement éclairé et exprès à la mise à disposition des informations sur Internet, tout en leur reconnaissant le droit de s'opposer à tout moment à la diffusion des informations²¹. Pour la diffusion via internet de la jurisprudence, la CNIL prône l'anonymisation des décisions de justice.

On verra plus en détail au point 5. la réponse des Etats européens à l'ensemble des risques découlant d'une publication des décisions de justice par internet, au nombre desquels figure le risque de détournement de finalité.

2.3. Des données pertinentes par rapport à la finalité

Selon l'article 4, § 1^{er}, c) de la directive 95/46, les données doivent être pertinentes, adéquates et non excessives au vu des finalités poursuivies. L'exercice de clarification des finalités attachées à la publication des décisions jurisprudentielles est donc essentiel puisqu'on ne peut traiter que les données nécessaires et adéquates pour atteindre les finalités annoncées. De la détermination des finalités découle la détermination des catégories de données pouvant faire l'objet du traitement.

La transparence de la justice implique en principe que soit mis à disposition du public le texte même des décisions prononcées par les cours et tribunaux, non expurgé de quelque données. Ce sont les greffes des tribunaux qui assurent la conservation de ces originaux intacts. Des exceptions sont admises dans tous les Etats européens, au nom desquelles même dans les greffes, le public ne peut accéder à certaines décisions ou ne peut accéder qu'à des décisions où est biffée l'identité des parties, afin de protéger des intérêts supérieurs tels ceux des mineurs, des victimes de délits sexuels, la sécurité nationale, l'intérêt de personnes concernées par une procédure en divorce, la confidentialité en matière de filiation et d'adoption, etc.

La finalité de diffusion du droit dans sa dimension jurisprudentielle nécessite-t-elle, quant à elle, que soit communiquée au public et aux professionnels du droit l'identité de toutes les

¹⁹ Résumé de l'avis accessible à l'adresse <http://bach.drt.garanteprivacy.it/garante/doc.jsp?ID=127839>

²⁰ Avis n° 07/96. En 1998, la refonte de la loi a apporté une réponse plus radicale à cette question puisque, à moins de s'inscrire dans le cadre d'une norme confiant la mission à l'autorité publique de publier ses/les décisions jurisprudentielles, seule la publication sous forme systématiquement anonyme est admise (voy. *infra*, point 5).

²¹ CNIL, 17^{ème} *Rapport d'activité 1996*, Paris, La Documentation française, 1997.

personnes intervenant aux procès ? De telles données sont-elles pertinentes et adéquates par rapport à l'objectif poursuivi ?

Puisqu'on a déjà dit que la publication des décisions de justice n'était pas la condition de leur publicité mais que, si elle ne représentait pas la garantie contre l'arbitraire des juges, elle y contribuait nécessairement, il est justifié de maintenir le nom des *acteurs publics* intervenant dans les décisions : le nom des juges et des représentants du ministère public. Cela correspond d'ailleurs à la pratique observée sur l'ensemble du continent européen : que les publications des arrêts et jugements se fassent au travers d'édition de revues papier ou sur support électronique, le nom des acteurs publics impliqués est la plupart du temps indiqué.

Qu'en est-il de la publication du nom des autres intervenants à la cause, spécialement les *parties* ? Ces données ne présentent qu'un lien de pertinence et de nécessité ténu par rapport aux finalités liées à la publication de la jurisprudence. Dans la grande majorité des cas, elles ne sont pas nécessaires à la compréhension de la cause et de son traitement par le juge²². Elles peuvent, certes, ainsi qu'il a été avancé par certains pourfendeurs de l'anonymisation, faciliter la mémorisation pour les étudiants et les praticiens du droit. La diffusion du nom des parties contribue-t-elle par ailleurs, comme la publication du nom des acteurs publics, à la transparence de la justice ? La transparence de la justice signifie la transparence de l'action des juges. Ce principe démocratique ne vise pas à faire porter à la connaissance de tous par le biais d'une publication générale le succès ou l'insuccès d'un justiciable dans ses prétentions juridiques. C'est à ce point vrai que c'est à titre de sanction ou de réparation que le juge peut ordonner une telle publication (dans les cas de condamnations pour diffamation, par exemple, ou pour concurrence déloyale). La publication de l'identité des parties ne participe donc pas dans la même mesure que la publication du nom des acteurs publics à la transparence de la justice. En somme, outre dans les cas où la publication est imposée comme sanction ou réparation, c'est dans les seuls cas où l'identité d'une partie est un élément clé de la décision (procès en destitution, par exemple) et ceux où une personnalité officielle est partie à une procédure liée à ou pouvant avoir des répercussions sur l'exercice de ses fonctions²³, qu'apparaît clairement justifiée la mention du nom des parties²⁴.

Notons encore que les données doivent être non seulement pertinentes par rapport aux finalités poursuivies par la publication, mais également « non excessives ». Cela signifie que, même si on devait estimer pertinent de diffuser le nom des intervenants au vu des finalités poursuivies par la publication de décisions de justice, les données personnelles ne peuvent être traitées (ici publiées) si elles sont excessives, c'est-à-dire si elles portent une atteinte trop importante aux droits des personnes concernées par rapport à l'intérêt de leur publication. C'est en fait le principe de proportionnalité qui intervient ici, principe qui fait l'objet des développements réservés au point suivant.

²² A ceux qui avancent que le remplacement du nom des parties par le rôle qu'elles tiennent (demandeur, défendeur, témoin) accentuerait le caractère difficilement lisible des décisions de justice, on rétorque volontiers qu'il y aurait sans doute davantage lieu de s'interroger sur l'opportunité du maintien de l'emploi par les juges d'une syntaxe et d'un langage surannés ou spécifiques, difficilement accessibles au commun justiciable, plutôt que de réduire les conditions de lisibilité des décisions prononcées à l'appellation des parties par leur nom. Aux Pays-Bas, en Allemagne, en Grèce, en Autriche, en Espagne, au Portugal, en Belgique, en Hongrie, etc., cela fait parfois des dizaines d'années que le public s'accommode sans difficulté de décisions où interviennent des acteurs plutôt que des personnes individualisées.

²³ Pour reprendre une exception au principe d'anonymisation admise par le régime juridique hongrois (voy. *infra*, point 5).

²⁴ Il y a également des cas où la publication des décisions est imposée par la loi aux fins par exemple de protéger des tiers (mise sous placement d'un conseil judiciaire, minorité prolongée,...)

On clôturera les considérations sur l'exigence de données pertinentes et non excessives en précisant que lorsqu'on conclut que l'identification des parties n'est pas pertinente par rapport aux finalités poursuivies par la publication de la jurisprudence, c'est bien sûr l'ensemble des données contribuant à cette identification qui sont visées et non pas les seuls noms et adresses, ainsi que le dit la CNIL²⁵, seule en son genre à préconiser une solution aussi irrationnelle²⁶.

3. L'application du principe de proportionnalité

Deuxième principe majeur intervenant dans la protection des données personnelles, le principe de proportionnalité découle directement de l'article 8 de la Convention européenne des droits de l'homme.²⁷ Cette disposition qui garantit la protection du droit au respect de la vie privée reconnaît le caractère non absolu de ce droit et admet des limitations à la protection pourvu, notamment, que ces atteintes ne soient pas disproportionnées. Cela signifie que l'on doit opter pour la voie la moins attentatoire au droit protégé. On ne peut en outre porter atteinte au droit protégé – ici par la publication d'informations apparaissant dans une décision de justice – si l'atteinte ainsi portée n'est pas compensée par un intérêt supérieur lié à une telle publication.²⁸

L'intérêt de publier les noms des parties lorsqu'on diffuse la jurisprudence peut se résumer en une aide à la mémorisation des cas et une contribution minimale à la transparence de la justice, à quoi on rajoutera certainement l'économie des frais et des délais induits par les manipulations nécessitées par l'anonymisation. Ces avantages pèsent-ils plus lourd que les atteintes causées par une publication via internet aux individus concernés ? Les atteintes peuvent, elles, être décrites en trois points : la perte de contrôle des données (réutilisations abusives), la négation du droit à l'oubli, et la nouvelle dimension de la publicité.

3.1. La perte de contrôle des données

²⁵ Délibération 01-057 du 29 novembre 2001, précitée.

²⁶ Les éléments à supprimer sont ceux qui permettent au public (et non aux seuls proches ou intimes) de reconnaître la personne en cause. Il se peut que, du fait de l'actualité judiciaire, le public puisse reconnaître aisément les personnes liées à un procès dont la presse s'est fait largement l'écho. Cela ne veut pas dire pour autant, comme le soutient la CNIL dans sa Délibération, que l'on doit renoncer à publier la décision de justice sous prétexte que sa lecture seule permettrait d'identifier les parties à la cause. Il faut considérer les éléments identifiants en faisant abstraction de l'actualité judiciaire (qui justifie que l'on connaisse le nom des personnes « faisant » cette actualité, sauf des victimes et des mineurs) qui ne vaut qu'un temps, et juger si vingt ans plus tard, les parties seraient encore reconnaissables par le public à la lecture du texte. Si oui, c'est vraisemblablement alors parce que les parties en cause sont des personnalités publiques (on sait vingt ans plus tard qui était le maire de Paris à telle époque). Or on a dit que si le jugement concerne une question présentant un lien ou une incidence sur l'exercice de l'activité publique de telles personnes, on ne devrait pas imposer de procéder à l'anonymisation de la décision.

²⁷ Dans son tout premier arrêt en matière de protection des données, la Cour de Justice des Communautés européennes a explicitement déclaré : « Aussi, pour les besoins de l'application de la directive 95/46, [...] importe-t-il de vérifier, en premier lieu, si une réglementation telle que celle en cause dans les affaires au principal prévoit une ingérence dans la vie privée et, le cas échéant, si cette ingérence est justifiée au regard de l'article 8 de la CEDH. » (C.J.C.E., arrêt du 20 mai 2003, *Österreichischer Rundfunk e.a.*, C-465/00, C-138/01 et C-139/01, § 72).

²⁸ Dans son arrêt *Österreichischer Rundfunk*, précité, la Cour européenne indique qu'il faut examiner si la disposition autrichienne en cause « est conforme à l'article 8 de la CEDH, au regard de l'exigence de proportionnalité, par rapport aux objectifs poursuivis » (§ 80). « Il convient, en ce sens, de mettre en balance l'intérêt de la république d'Autriche à garantir une utilisation optimale des fonds publics [...] avec la gravité de l'atteinte au droit des personnes concernées au respect de leur vie privée » (§ 84).

Il a déjà été signalé au point 2.2. que le support électronique offre des possibilités de recherche et d'utilisation des informations inenvisageables dans le contexte du papier, à tout le moins à une telle échelle et avec une telle efficacité. Et que cela signifie autant de tentations d'effectuer, à partir d'une base de données jurisprudentielles, des recherches sur des personnes plutôt que sur des cas. Le phénomène des réseaux rendant ces bases de données accessibles à tout moment de tous les bureaux et les salons accentue évidemment ces risques.

Le danger des réutilisations détournées et abusives tient surtout dans le profilage des individus. Il ne s'agit pas tant, à ce jour, d'entrevoir la création de casiers judiciaires²⁹ privés, étant donné que la publication des décisions de justice même sur support numérique est encore loin de couvrir l'ensemble des décisions de l'ensemble des juridictions. On ne peut prétendre reconstituer à partir des bases de données jurisprudentielles disponibles, tout le passé judiciaire d'un individu. Il s'agit bien davantage de craindre les discriminations et les préjugés qui s'appuieraient sur le relevé d'information judiciaire même partielle.

Étant donné le caractère international d'internet, les flux transfrontières des données sont inhérents à son fonctionnement, ce qui ajoute au risque de réutilisation incontrôlée des données, le risque que les données soient traitées dans des pays n'offrant aucune protection.

3.2. La négation du droit à l'oubli

Le droit à l'oubli du passé judiciaire est un droit largement reconnu dans nos démocraties.³⁰ Il a pour objet « d'assurer la protection du passé du sujet en permettant à ce dernier de s'opposer à l'exhumation de faits appartenant à un épisode de sa vie que le temps a rendu secret »³¹. Garantir le droit à l'oubli c'est prendre en compte le fait que tout individu peut évoluer et s'amender et qu'une fois payé la dette à la société, cette dernière doit offrir la possibilité de se réinsérer et de redémarrer sans porter toute la vie le poids des erreurs du passé. L'amnistie est une consécration juridique particulière du droit à l'oubli. La limitation de la durée de conservation des données personnelles imposée par la législation de protection des données en est une autre. Les données ne peuvent être conservées sous une forme nominative qu'autant qu'elles sont nécessaires à l'accomplissement de la finalité poursuivie³². Au-delà, elles doivent être effacées ou anonymisées.

Le droit à l'oubli s'oppose au droit à l'information, avec le facteur temps comme critère de résolution du conflit. Le droit à l'oubli doit céder devant les exigences du droit à l'information lorsque les faits divulgués présentent un intérêt contemporain à la divulgation³³. Ainsi, lorsque la décision prononcée par une juridiction s'inscrit dans l'actualité judiciaire, il est légitime de l'évoquer en mentionnant le nom des parties (à l'exclusion des victimes et des

²⁹ C. Bourgeois propose avec pertinence de parler de casiers juridiques plutôt que judiciaires étant donné que ces derniers sont limités à la mention des condamnations pénales alors que les autres englobent les décisions de toute nature (*op. cit.*, p. 17)

³⁰ Sur ce droit, voy. notamment : C. COSTAZ, « Le droit à l'oubli », *Gaz. Pal.*, 1995, Doctr., pp. 961 et s. ; R. LETTERON, « Le droit à l'oubli », *Revue de Droit Public et de la Science Politique*, 1996, vol. 112, n° 1-3, pp. 388 et s. ; A. STROWEL, « Les conditions d'exercice du droit à l'oubli : liberté d'informer et droit à l'oubli », *Légipresse*, 1998, n° 154, pp. 126 et s. ; R. DUASO-CALES, *op. cit.*, pp. 86 et s.

³¹ C. COSTAZ, *op. cit.*, p. 963.

³² Art. 6, § 1^{er}, e), de la directive 95/46.

³³ Et à condition que la divulgation des faits soit licite. Voy. R. LETTERON, *op. cit.*, pp. 413-414 ; A. STROWEL, *op. cit.*, p. 126 ; R. DUASO-CALÈS, *op. cit.*, p. 90.

mineurs). Par contre, dès lors que les nécessités de l'actualité ne justifient plus une redivulcation, c'est le droit à l'oubli qui prend le pas et toute nouvelle publication de la décision avec mention des personnes impliquées est fautive. Le droit à l'information l'emportera malgré l'écoulement du temps pour les seuls faits relevant de l'histoire (les jugements relatifs à de grands criminels, par exemple) et pour ceux concernant les activités publiques de personnalités publiques.

Or, la publication de la jurisprudence via internet ne respecte pas l'équilibre atteint entre droit à l'oubli et droit à l'information. Le stockage illimité des informations sur le réseau les rend accessibles de façon constante, longtemps après le moment où leur diffusion était justifiée par les impératifs du droit à l'information.

L'affichage permanent en quelque sorte qui résulte des caractéristiques d'internet correspond à « une sorte de peine complémentaire perpétuelle »³⁴.

Aux limites de la mémoire humaine, internet oppose aujourd'hui l'infailibilité de la « mémoire totale »³⁵. Or, « la mémoire peut aussi être celle de la rancune, de la vengeance, du dénigrement. Grâce à sa mémoire totale, Internet préserve les mauvais souvenirs, les erreurs passées, les écrits que l'on aimerait renier plus tard. [...] La transparence des informations sur les erreurs de trajectoire, les condamnations, les modes de vie de certains pourraient affecter et troubler la vie d'autres membres de la parenté. Des rapprochements malheureux ou malhonnêtes deviennent très faciles sur le Net. Ils pourront être utilisés par quiconque veut mettre son prochain en difficulté. »³⁶

Des institutions juridiques telles la réinsertion et la réhabilitation risquent d'être vidées de leur sens dans ce contexte ou d'être à tout le moins affaiblies.

3.3. La nouvelle dimension de la publicité

Il existe différents degrés de publicité et l'on ne peut les tenir pour équivalents. Il s'ensuit que l'on ne peut se prévaloir de la publicité accordée à des informations pour légitimer toute forme de publicité de ces informations.

Lorsqu'elle emprunte la voie d'internet, de locale, la publicité devient globale, et de médiate, immédiate. Cela signifie pour les personnes concernées par les informations un enjeu d'une autre envergure pour leur vie privée.

Par ailleurs, une publicité « disséminée » n'est pas de même nature qu'une publicité « rassemblée ». La deuxième fait naître plus de risques pour les personnes concernées par les données. Ainsi, avoir accès aux minutes des procès auprès des greffes des tribunaux, c'est-à-dire en des lieux dispersés, n'a pas la même valeur, et ne présente pas les mêmes dangers pour la vie privée des personnes citées, que d'avoir accès à une base de données rassemblant l'ensemble des décisions prononcées par les tribunaux du pays.

A titre d'illustration, il est intéressant de mentionner la décision adoptée par la Cour suprême américaine saisie d'une affaire dans laquelle un journaliste demanda au *Federal Bureau of Investigation* à avoir accès aux documents concernant les arrestations, inculpations et

³⁴ E. LESUEUR DE GIVRY, « La question de l'anonymisation des décisions de justice », <http://www.courdecassation.fr/rapport/rapport00/etudes&doc/LESUEUR.htm>

³⁵ ...pour reprendre une expression aujourd'hui partagée par la doctrine.

³⁶ D. ETTIGHOFFER, « Les droits de l'homme numérique : le droit à l'oubli », 2, <http://www.eurotechnopolis.org/fr/oubli.html>

condamnations dont firent l'objet quatre individus³⁷. Les arrestations, inculpations et condamnations sont des événements publics retranscrits dans les fichiers publics tenus par les tribunaux. Pour le seul vivant des quatre individus ciblés par le journaliste, le F.B.I. refusa de transmettre l'information qu'il détenait sous forme compilée, estimant que la communication porterait atteinte à la vie privée de l'individu en question. La Cour suprême soutint à l'unanimité cette argumentation. Elle rejeta l'argument retenu par la Cour d'appel, selon lequel il n'y a plus de « privacy interest » en présence d'informations déjà rendues publiques. Pour la Cour, il y a une importante différence entre une communication « éparpillée » de fragments d'information et la divulgation de l'information dans son ensemble. « But the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, country archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information. »³⁸

Et quoi de moins accessible que le casier judiciaire, composé pourtant d'informations publiques ?

3.4. La nécessité d'un nouvel équilibre

Il est clair que les nouvelles technologies font naître des risques nouveaux pour les personnes concernées par les données. Le point 114 du Livre vert de la Commission européenne sur l'information émanant du secteur public dans la société de l'information, souligne très clairement que « l'émergence de la société de l'information pourrait poser de nouveaux risques pour la vie privée des individus si des registres publics venaient à être accessibles sous forme électronique (en particulier en ligne et sur Internet) et dans de larges quantités »³⁹.

Là où une publicité existait déjà dans le monde papier, on avait pu atteindre un équilibre entre protection de la vie privée et protection d'autres intérêts. Or, la publication numérique « engendre des risques en matière de protection des données sans commune mesure avec ceux liés aux modes traditionnels d'accès ou de publication de la jurisprudence »⁴⁰.

En définitive, les nouveaux risques liés à une publication via internet se résument en une accessibilité des informations indépendante du lieu, des frontières et du temps ; une conservation longue durée (« the eternity effect »⁴¹) : la mémoire électronique ne permet plus le droit à l'oubli ; des utilisations secondaires incontrôlées des informations ; le profilage des individus.

³⁷ *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989).

³⁸ 489 U.S., 764. Voy. également la décision d'une Cour d'appel de Californie dans l'affaire *Westbrook v. Los Angeles County* (32 Cal. Rptr. 2d 382 (Cal. App. 1994)) dans laquelle un éditeur avait demandé à recevoir une copie d'une disquette contenant les décisions d'une *municipal court* en matière pénale. La Cour refusa la communication de la compilation : « There is a qualitative difference between obtaining information from a specific docket or on a specified individual, from obtaining docket information on every person against whom criminal charges are pending in the municipal court. [...] It is the aggregate nature of the information which makes it valuable to respondent ; it is the same quality which makes its dissemination constitutionally dangerous ».

³⁹ *L'information émanant du secteur public : une ressource clé pour l'Europe*, COM(1998)585, Luxembourg, Office des publications officielles des Communautés européennes, 1999, p. 17.

⁴⁰ Y. POULLET, *op. cit.*, p. 71.

⁴¹ S. WALZ, *op. cit.*, p. 3.

Créant de nouveaux dangers pour la vie privée des individus et leur maîtrise de leur image et de leur réputation, les technologies modifient l'équilibre atteint dans un contexte traditionnel. Les conditions d'un nouvel équilibre entre les intérêts contradictoires en présence doivent en conséquence faire l'objet d'une nouvelle évaluation. Cette évaluation a déjà été effectuée par nombre d'Etats européens. Ils y sont invités tant par le respect du principe de proportionnalité que par le régime de protection plus strict que la directive réserve aux données « judiciaires ».

4. Le régime plus strict des données « judiciaires »

La directive accorde un régime de protection plus strict pour les catégories de données considérées comme sensibles, au rang desquelles figurent les données « relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté »⁴². Les Etats membres peuvent élargir cette catégorie aux données relatives aux jugements civils et aux sanctions administratives. Le traitement de ces données, que par commodité on qualifie de « judiciaires », ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national.

S'ils veulent permettre la publication numérique de décisions de justice qui ne soit pas le seul fait de l'autorité publique (que ce soit une publication massive ou même la publication d'une décision isolée), les Etats membres sont donc tenus de prévoir des garanties appropriées. Si une publication est effectuée « aux seules fins de journalisme ou d'expression littéraire ou artistique »⁴³, elle pourra toutefois bénéficier des exemptions mises en place par chaque Etat membre pour ménager un juste équilibre entre protection de la vie privée et liberté d'expression. La presse est donc légitimée, dans la plupart des pays de l'Union européenne, à diffuser des données « judiciaires » par la voie d'internet (pourvu qu'elle respecte les autres exigences de la législation de protection des données dont elle n'est pas exemptée, notamment les limites de durée de conservation⁴⁴).

5. Les garanties mises en place par les Etats membres de l'Union européenne⁴⁵

Sommés donc, à la fois par le principe de proportionnalité⁴⁶ et par le régime spécifique des données judiciaires⁴⁷, d'entourer de garanties le traitement (ici la publication numérique) des données judiciaires, les Etats membres de l'Union européenne ont mis en place des régimes

⁴² Art. 8, § 5, de la directive 95/46.

⁴³ Art. 9 de la directive 95/46.

⁴⁴ A titre d'exemple, au Danemark, les médias ne sont pas autorisés à maintenir dans des bases de données accessibles au public des données concernant des particuliers au-delà de 3 ans après l'événement qui a donné lieu à leur enregistrement, à moins que l'accès à ces données présente un intérêt public tel que la liberté d'information doit l'emporter sur le droit des personnes à l'anonymat.

⁴⁵ Les lignes qui suivent s'appuient notamment sur les informations fournies par 15 Etats membres et rassemblées dans le document 9370/04 JURINFO 9 du Conseil, du 8 juin 2004, ayant pour objet le droit à l'anonymat lors du traitement de données par la justice. Ce document est venu en réponse à un questionnaire de la délégation italienne qui souhaitait comparer la façon dont le principe du droit à la vie privée était appliqué en matière d'informatique juridique dans les différents Etats membres.

⁴⁶ Qui n'admet comme licite, quel que soit le diffuseur, que la publication de données qui sert un intérêt supérieur à l'atteinte qu'elle fait encourir aux personnes concernées.

⁴⁷ Qui impose de prévoir des garanties lorsque la publication de données judiciaires ne s'effectue pas sous le contrôle d'une autorité publique.

juridiques qui, à leurs yeux, rétablissent l'équilibre entre intérêt servi par la publication et atteinte portée aux droits des personnes citées dans les décisions.

Sur les dix-sept pays à propos desquels l'information était disponible, on constate un large consensus pour l'instauration de l'anonymat indépendamment de la demande des parties comme règle générale pour les personnes physiques non professionnelles intervenant dans les décisions de justice. C'est le choix posé par l'Allemagne, l'Autriche, la Belgique, l'Espagne, la Finlande, la France, la Grèce, la Hongrie, les Pays-Bas, la Pologne, le Portugal et la République tchèque⁴⁸. Une anonymisation partielle est mise en place au Danemark, en Italie, en Suède et à la Cour de Justice des Communautés européennes ainsi qu'au Tribunal de première instance. L'Estonie tergiverse tandis que le Royaume-Uni est le seul à ne pas souhaiter modifier sa tradition de diffusion, en principe sans restriction, du nom des personnes impliquées dans les procédures judiciaires.

Il est à noter que dans tous les Etats qui ont opté pour l'anonymisation systématique en cas de publication, le prononcé public des décisions contient les données identifiantes (telles les noms, prénoms, adresses, dates de naissance, numéros d'identification,...), de même que les exemplaires des décisions conservés aux greffes des tribunaux et publiquement accessibles, sauf exceptions prévues par la loi. Seule la publication ou seule la publication numérique, se voit appliquer la règle de l'anonymat.

L'anonymisation s'effectue partout par la suppression de toutes les données permettant l'identification des personnes et le remplacement par des initiales ou par le rôle joué dans la procédure. La CNIL française est la seule à avoir prôné la simple suppression des noms et adresses⁴⁹. Elle est aussi la seule à avoir considéré qu'on était plus à l'abri des dérives en présence de bases de données payantes, et qu'en conséquence l'anonymisation n'était pas requise pour ces bases de données-là, la suppression de la mention des adresses des parties étant suffisante. Cet argument n'a convaincu aucun autre Etat, l'accès payant ne signifiant pas que l'accès serait nécessairement restreint à des utilisateurs scrupuleux, soucieux de respecter la finalité de la publication. On a vu d'ailleurs que l'atteinte pour les personnes citées dans les décisions n'étaient pas limitée aux utilisations abusives des données⁵⁰. Il n'y a donc dans aucun autre pays de différence de traitement entre bases de données payantes et celles librement accessibles sur internet.

En Allemagne et en Grèce, l'anonymisation systématique des décisions destinées à être publiées a d'abord été « de longue tradition » en Allemagne, et « de tradition depuis 1945 » en Grèce, avant d'être étayée par les législations de protection des données adoptées sur la base de la directive 95/46.

Aux Pays-Bas, c'est pour éviter de devoir évaluer les situations au cas par cas, qu'il est prévu, par principe, que toutes les décisions judiciaires doivent être rendues anonymes en cas de publication.

En Belgique, hors sous le contrôle d'une autorité publique et à condition que cela entre dans l'exercice de ses tâches, la publication des données judiciaires est interdite depuis la modification de la loi en 1998 pour la mettre en conformité avec la directive. La définition de ces données est singulièrement large puisqu'elle couvre les données relatives à des litiges

⁴⁸ Affirmer comme certains (F. LEPLAT, « Décisions de justice publiées sur Internet : pour le droit à l'anonymisation sur simple demande », <http://www.droit-technologie.org>, 10 mai 2002 ; C. BOURGEOS, *op. cit.*, p. 17) que l'anonymisation des décisions est l'exception et ne prévaut que dans 3 pays européens ne correspond assurément pas à la réalité juridique européenne.

⁴⁹ Voy. *supra* point 2.3. Cette solution a été érigée en règle dans l'arrêté du 9 octobre 2002 relatif au site Internet de Légifrance.

⁵⁰ Voy. *supra* point 3.

soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté. Cela signifie que l'ensemble de la jurisprudence ne peut être publié qu'après anonymisation à moins que la publication ne soit nécessaire à l'exercice des tâches d'une autorité publique et effectuée sous son contrôle. Pour le site internet officiel par lequel le ministère de la Justice publie la jurisprudence de la Cour de cassation et des principales juridictions du pays, il a ainsi été procédé à l'anonymisation des décisions. La publication des arrêts du Conseil d'Etat via le Web a été réalisée avant la modification de la loi et est la seule couverte par un arrêté royal la prévoyant spécifiquement. Cet arrêté unique en son genre stipule que la dépersonnalisation des arrêts publiés s'effectue à la demande des parties et que les arrêts concernant l'accès au territoire ne sont pas publiés.

Dans plusieurs des pays exigeant l'anonymisation, des exceptions à cette démarche sont admises. Il en est ainsi pour les décisions dont la publication est imposée à titre de sanction ou de réparation d'un comportement illicite (en cas de condamnation pour diffamation ou concurrence déloyale, par exemple) afin de permettre à la victime d'informer le public de l'infraction commise par la partie condamnée ; ou si le maintien des données personnelles est nécessaire à la compréhension de la décision. En Hongrie, « la plus importante de ces exceptions a trait aux affaires qui touchent à des questions d'intérêt général importantes, par exemple lorsqu'une personnalité officielle est partie à une procédure pour des motifs liés à l'exercice de ses fonctions. Dans ce cas, on peut estimer que l'intérêt du citoyen à obtenir des informations sur l'affaire l'emporte sur l'intérêt personnel des parties »⁵¹.

L'Italie comme les deux juridictions communautaires ne procèdent à l'anonymisation qu'à la demande d'une partie ou si la juridiction le décide elle-même. En Italie, en outre, certaines matières font l'objet d'une anonymisation systématique : les affaires concernant le droit familial et l'état civil, et il est interdit de faire apparaître le nom des mineurs.

Au Danemark, si l'anonymat lors de la publication des décisions n'est pas la règle générale, il est quand même d'application dans nombre de situations. Ainsi, les particuliers ne sont pas autorisés à publier des décisions judiciaires sans le consentement explicite des personnes concernées ou à moins que cela ne soit nécessaire à l'exécution d'une mission effectuée dans l'intérêt public. Par ailleurs, pour la mise en œuvre de systèmes d'information juridique, des règles ont été édictées par l'Agence pour la protection des données. Cette autorité de contrôle a décidé que la publication des décisions judiciaires requiert l'anonymat dans un certain nombre de situations : notamment les affaires pénales, matrimoniales et fiscales ainsi que les actions en indemnisation. La loi interdit de surcroît la divulgation de l'identité des personnes impliquées dans les affaires de garde, de paternité et d'adoption.

En Suède, une loi en vigueur depuis le 1^{er} décembre 2004 stipule que le système d'information juridique mis en place par l'Etat ne peut contenir de données faisant directement référence à une personne physique vivante (avec une interdiction spécifique de faire apparaître les numéros nationaux d'identification), à moins qu'il ne s'agisse de juges ou d'experts ou de références à de la littérature. Les autres publications de la jurisprudence sont, quant à elles, simplement soumises à la loi relative à la protection des données. Si elles sont le fait des tribunaux et si cela relève de leurs tâches, les publications de données à caractère personnel sont autorisées. Pour les bases de données juridiques privées, une mise en balance doit être effectuée. Si leur responsable est couvert par la loi relative à la liberté d'expression, il échappe à la législation de protection des données et peut librement publier les données qu'il souhaite, sous réserve de répondre d'éventuelles infractions à la loi sur la liberté d'expression.

⁵¹ Document 9370/04 JURINFO 9 du Conseil, *op. cit.*, p. 29.

En Estonie, il semble que la réflexion sur le sujet est lancée mais n'a pas encore abouti car, alors que l'inspection estonienne de la protection des données a proposé de remplacer, sur le site internet, les noms des personnes citées dans les décisions par des initiales, aucune modification n'a encore été observée.

Comme évoqué plus haut, le Royaume-Uni se situe dans une position diamétralement opposée à la majorité du groupe d'Etats membres. Son attachement à la règle de diffusion du nom de toutes les personnes impliquées dans les procédures judiciaires est justifié notamment par le fait que « les systèmes juridiques de la 'common law', fondés sur la règle du précédent [...] accordent bien plus d'importance aux décisions des tribunaux que les juridictions qui fondent leurs décisions sur des codes écrits »⁵². La règle de diffusion des noms des parties ne souffre aucune restriction « sauf s'il y a de bonnes raisons pour cela »⁵³.

⁵² *Ibid.*, p. 72.

⁵³ *Ibid.*